3.4 Verhoog het rendement op beveiligingsuitgaven met periodieke analyses

Beveiliging van informatievoorziening is een complex en ondoorzichtig probleem. Het is dan ook een zorgpunt voor veel organisaties. Fraude en inbraak zijn vrijwel dagelijks nieuws in de media. De zorgen worden meestal niet kleiner, ondanks grote inspanningen in de vorm van omvangrijke doorlichting van infrastructuur en organisatie. De resultaten kunnen aanzienlijk verbeterd worden als beveiliging in 'behapbare' brokken wordt benaderd. Dit artikel gaat in op deze stelling. Beschreven wordt een procesgestuurde methode van security-auditing.

Auteurs: **Iwan van Ophem**, **Dennis Joosten**. Ir. Iwan van Ophem is ICT security consultant en ir. Dennis Joosten is systeemarchitect. Zij zijn werkzaam bij Ordina Finance Business Solutions.

In vergelijking met de periode 1960-1990, is er in het laatste decennium ontzettend veel gebeurd op het gebied van systeemintegratie. De groei van Internet in die periode is daar in belangrijke mate debet aan. Onderzoekers verwachten dat binnen enkele jaren 'alles met alles' communiceert [1]. Dit is niet alleen van toepassing binnen de organisatiegrenzen; ook klanten en partners krijgen toegang tot data via dedicated applicaties, vaak via Internet. De verschuiving van product- naar klantgerichte organisaties en systemen heeft ervoor gezorgd dat nieuwe infrastructuren zijn geïmplementeerd met als doel: applicaties via het nieuwe kanalen aanbieden voordat anderen hetzelfde doen. Kortom:

- nieuwe technologie;
- een spinnenweb van gekoppelde systemen en applicaties;
- veel ingangen naar data, die welig stromen door de gekoppelde systemen;
- dit alles in relatief korte tijd gerealiseerd.

De ontwikkelingen en de bijbehorende risico's zijn in veel gevallen wel onderkend: met behulp van richtlijnen (policy's) en (infrastructurele) maatregelen is getracht beveiliging te realiseren. Beveiliging is echter niet alleen een puur infrastructureel probleem of een eenmalige actie, maar een voortdurend proces van acteren, controleren en verbeteren. De automatisering gaat immers ook continu door, net als de ontwikkeling van inbraaktechnieken. De bestaande oplossingen zijn meestal momentopnamen: omvangrijke audits, die door de complexiteit van de omgeving niet opleveren wat beoogd is – behalve rapporten die in de kast verdwijnen [2]. Dit is te voorkomen door auditing op kleinere schaal in te richten, het analysedomein op te delen in meerdere kleine domeinen en met een geregelde frequentie deze kleine domeinen aan een onderzoek te onderwerpen.

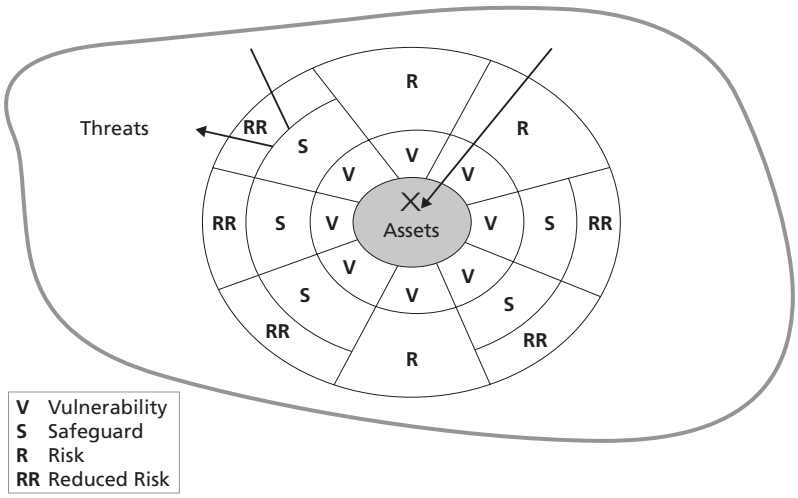
We beschrijven een procesgestuurde methode van security-auditing, waarbij de waardevolle gegevens in de organisatie als uitgangspunt genomen worden. De compacte methode is in relatief korte tijd uit te voeren. Door dit frequent te doen, wordt afgestapt van beveiliging als momentopname, maar sluit deze aan bij de praktijk.

De onderliggende theorie

ICT security (informatiebeveiliging) heeft als doel het beschermen van waardevolle assets (elektronische informatie). Assets hebben een drietal kwaliteitsaspecten, die door externe factoren (negatief) beïnvloed kunnen worden [3].

1 *Beschikbaarheid*: de eigenschap dat informatie beschikbaar en 'bruikbaar' is op het moment van opvragen.
2 *Integriteit*: de eigenschap dat informatie niet ongeautoriseerd veranderd of verwijderd kan worden.
3 *Vertrouwelijkheid*: de eigenschap dat informatie niet beschikbaar gesteld wordt of onthuld wordt aan ongeautoriseerde personen.

ICT security tracht deze kwaliteitsaspecten op peil te behouden. Elk aspect is in zijn omgeving onderhevig aan specifieke bedreigingen (*threats*). Het Security Wiel van *Michiels* [4] (zie figuur 1) laat dit zien: de zwakke plekken (vulnerabilities) van een asset worden mogelijk uitgebuit door deze threats, met als doel de kwaliteitsaspecten aan te tasten. Er bestaat in dat geval een beveiligingsrisico (risk). Als er een risico bestaat en dit een ontoelaatbaar gevolg heeft, kunnen er beveiligingsmaatregelen (safeguards) getroffen worden. Safeguards hebben als doel het beveiligingsrisico te verkleinen tot een acceptabel niveau. Er ontstaat dan een gereduceerd risico (reduced *r*isk). Een beter resultaat is niet mogelijk, want 100% beveiliging



Figuur 1 Security- wiel.

is feitelijk een utopie. In de figuur is dan ook te zien dat sommige threats nog steeds vulnerabilities kunnen uitbuiten. Er bestaat dan blijkbaar een acceptabel risico – of: nog onbekend risico –, terwijl andere onacceptabele risico's gereduceerd zijn door safeguards. Figuur 1 vormt de basis voor de periodieke analyse en zal als referentie dienen bij het uiteenzetten van het analyseproces.

Periodieke analyse

Een belangrijk resultaat van de periodieke analyse is het aangeven van prioriteiten van de beveiligingsstappen die moeten worden ondernomen voor de aangetoonde onacceptabele risico's. Mede hierdoor levert het frequent uitvoeren van de analyse een stuurmiddel op voor de bedrijfsvoering van de (ICT-)beveiliging (op de korte en middellange termijn).

De prioriteit van beveiliging van een asset wordt tweeledig bepaald:
1 enerzijds door de stakeholders toegekende waarde aan een asset;
2 anderzijds door het uit analyse aangetoonde bestaan van beveiligingsrisico's voor een asset.

Hieronder worden twee onderdelen van de periodieke analyse beschreven:
1 de classificatiemethode waarmee de waarde van een object bepaald wordt,
2 en het proces waarmee de (onacceptabele) beveiligingsrisico's bepaald worden.

I- De classificatiemethode

De periodieke analyse maakt gebruik van kwalitatieve classificatie. Dit betekent dat de waarde, maar ook de beveiligingsrisico's worden uitgedrukt door middel van hoog-laagclassificaties (bijvoorbeeld: laag, middel en hoog). Een onderscheid van meer dan 4 of 5 niveaus is in de praktijk vaak niet meer zinvol [2]. Voordelen van deze classificatiemethode is dat ze vlot, inzichtelijk en begrijpelijk is; daarnaast geldt dat bij systemen die nog in de ontwikkelfase zitten, een kwantitatieve analyse vaak niet mogelijk is.
In deze scan wordt de BIV-classificatiemethode gehanteerd.
BIV staat voor Beschikbaarheid, Integriteit en Vertrouwelijkheid, de fundamentele drie-eenheid van de informatiekwaliteit, zoals uiteengezet bij het security-wiel. De BIV-classificatie geeft voor elk van deze drie fundamenten het belang van behoud of waarde aan. De schaal voor elk van de fundamenten loopt van 1, minder belangrijk, tot 3, zeer belangrijk. Een voorbeeld van een BIV-classificatie voor de waarde van een database met authenticatiegegevens zou kunnen zijn: 2, 3, 3 (beschikbaarheid is belangrijk en integriteit en vertrouwelijkheid zijn zeer belangrijk). Dit geeft dan de waarde van de authenticatiedatabase weer, vooral ten opzichte van andere systemen (prioriteit!). De kwalitatieve score wordt bepaald op basis van een aan de stakeholders verstrekte vragenlijst. Een dergelijke vragenlijst dient wel afgestemd te worden op de bedrijfs- en/of systeemcontext.

II – De risicoanalyse

De risicoanalyse bestaat uit zeven stappen, gebaseerd op ISO 13335 – part III [5]. In deze zeven stappen worden de assets, vulnerabilities, threats en uiteindelijk de risico's uit het security-wiel bepaald. Het resultaat van deze analyse is een lijst van (onacceptabele) risico's, met een onderscheid op basis van prioriteiten. Met het resultaat van deze scan komt voldoende informatie beschikbaar voor een gestuurde en resultaatgerichte selectie van safeguards om de risico's te reduceren. Sturen kan door middel van de prioriteiten, en safeguard-keuze door inzicht in de bedreigingen. In de analyse wordt op meerdere momenten gebruik gemaakt van kwalitatieve classificatie. Hieronder worden de zeven stappen waar de risicoanalyse uit bestaat beschreven. Een toepassing van deze analyse is onder meer te vinden in *Van Ophem* [3].

1 Identificatie van het businessdomein

Deze stap heeft twee doelen:

- afbakening van het systeemdomein;
- identificatie van relevante stakeholders binnen dit domein.

Bij complexe informatiesystemen is vaak niet duidelijk op welke organisatieonderdelen invloed uitgeoefend wordt. In de domeinafbakening van het systeem moet bepaald worden welke organisatieonderdelen betrokken worden bij de analyse. Bij erg complexe systemen kan het ook raadzaam zijn het systeem zelf in stukken op te delen alvorens het domein te bepalen. Verder is het belangrijk te weten wie de stakeholders van het systeem(deel) zijn. Het is daarbij van belang een inschatting te maken welke stakeholders relevante informatie in het auditproces kunnen leveren.

2 Identificatie van de assets

In de deze stap worden de assets binnen een geselecteerd domein geïdentificeerd. De relevante stakeholders en aanwezige systeemdocumentatie kunnen hierbij helpen.

Het is raadzaam de assets te groeperen: gegevens die op een zelfde niveau zitten (voorbeelden: klantgegevens, financiële gegevens, persoonlijke gegevens) zullen vaak hetzelfde risicoprofiel hebben, en dus ook een oplossingsrichting gemeen hebben. Daarnaast is het verstandig onderscheid te maken tussen gegevens die zich 'verplaatsen' via een (elektronisch) netwerk en gegevens die met name liggen opgeslagen in een database. Hierbij is vaak ook een verschil in granulariteit te zien (een verzameling versus bijvoorbeeld data met betrekking tot één polis of persoon).

3 Waardebepaling

In deze stap wordt elke geïdentificeerde asset op een kwalitatieve manier (bijvoorbeeld de BIV-classificatie) gewaardeerd door de relevante stakeholders. De kwalitatieve waardebepaling vindt plaats op basis van een vastgestelde lijst van criteria, die mede wordt bepaald op basis van de door stake-

holders ingegeven belangen. De waarde van een asset is een belangrijke graadmeter in de risicobepaling. De andere twee graadmeters, de mate van bedreiging en de gevoeligheid van de assets voor deze bedreiging, worden in de volgende twee stappen bepaald.

4 *Identificatie van bedreigingen*
Een bedreiging kan gezien worden als een samenloop van omstandigheden met de potentie om een asset schade te berokkenen. Doel van deze stap is bedreigingen van de assets kwalitatief te beoordelen naar hun impact. Om dit proces te versnellen, bestaat voor gedistribueerde systemen een aftelbare lijst met bedreigingen (zie kader). Het is belangrijk in deze stap geen rekening te houden met reeds bestaande beveiligingsmaatregelen. Gebeurt dit wel, dan bestaat de mogelijkheid dat men van bedreigingen ten onrechte constateert dat die afdoende zijn afgewend. Het is ook in deze stap raadzaam de stakeholders te betrekken, omdat zij vaak een goede inschatting kunnen maken van de impact die verschillende bedreigingen op hun gegevens hebben.

5 *Identificatie zwakke plekken*
De kwetsbaarheid van een asset geeft de mate weer waarin een bedreiging 'succesvol' kan zijn voor een asset. Digitale gegevens zijn bijvoorbeeld gevoeliger voor modificatie dan gegevens op papier. Ook hier is raadzaam gebruik te maken van een kwalitatieve aanduiding met behulp van de stakeholders. Belangrijk is ook hier geen rekening te houden met eventuele bestaande beveiligingsmaatregelen.

6 *Identificatie van bestaande beveiligingsmaatregelen*
In deze stap worden de reeds bestaande beveiligingsmaatregelen geïdentificeerd. Deze maatregelen kunnen uiteenlopen van encryptietechnieken en firewalls tot fysieke beveiliging (gesloten deuren) en policy's (regelgevingen). Deze stap wordt bij de risicobepaling buiten beschouwing gelaten. Na de audit is deze informatie relevant om te bepalen of de bestaande maatregelen nog voldoen, een aanpassing behoeven of geheel vernieuwd moeten worden.

7 *Risicobepaling*
Op basis van de eerste vijf stappen van deze analyse valt voor elke asset een risicogetal per bedreiging te bepalen. Uiteenlopende meetmethoden zijn hiervoor bruikbaar. In tabel 1 wordt een voorbeeld gegeven van een kwalitatieve meetmethode. Te zien is hoe een asset met een in stap 3 geclassificeerde gemiddelde waarde en met een in stap 4 hoog geclassificeerde bedreiging voor denial of service-aanvallen (DoS'en) en een gemiddeld geclassificeerde gevoeligheid hiervoor, een totaal risicogetal krijgt van 4. De gearceerde cellen geven aan wanneer er sprake is van een onacceptabel risico. Deze asset heeft dus een onacceptabel risico voor DoS'en. Als prioriteitswaarde heeft deze asset ook een waarde van 4. Andere onacceptabele

risico's kunnen een lagere prioriteit hebben (3) of een hogere (5,6). Op basis hiervan en het eventueel aanwezige bedrijfsbeleid voor beveiliging, kan de bedrijfsvoering in beveiliging nu gestuurd worden.

In de conclusie worden aanbevelingen gedaan over vervolgstappen op deze analyse.

	Mate van bedreiging:	Laag			Gemiddeld			**Hoog**		
	Gevoeligheid:	L	G	H	L	G	H	L	**G**	H
Waarde van de Asset:	Laag	0	1	2	1	2	3	2	3	4
	Gemiddeld	1	2	3	2	3	4	3	**4**	5
	Hoog	2	3	4	3	4	5	4	5	6

Tabel 1 Denial of service-risico voor een asset.

Domeinmodellen

De periodieke analyse begint met het bepalen van het domein waartoe de gegevens behoren. De analyse kan toegespitst worden op het domein waarin de methode wordt toegepast. In dat geval spreken we van een domeinmodel. Een domeinmodel is een blauwdruk van het domein, waarin reeds een invulling is gemaakt van groeperingen van assets of individuele assets, BIV-coderingen – afhankelijk van de plek van de data in de organisatie – gebruikersgroepen en de granulariteit van de dataverzameling. Bijvoorbeeld: in het verzekeringsdomein komen assets voor als offertes, overeenkomsten en grootboek. De blauwdruk zorgt voor een versnelde analyse van de risico's doordat meteen tot de analyse kan worden overgegaan, zonder dat de situatie vanaf 'scratch' in kaart moet worden gebracht. Templates van vragenlijsten en een lijst van mogelijke bedreigingen kunnen het gebruik van de methode verder versnellen: het uitvoeren van de analyse wordt een eindig proces in plaats van een eindeloze brainstorm. Uiteraard kan een organisatie een domeinmodel op maat voor de eigen organisatie maken. Als het model beheerd wordt, zodat wijzigingen in de situatie worden opgenomen, kan de analyse in korte tijd worden afgerond.

Conclusie

In dit artikel hebben we getracht handvatten te geven om de problemen te lijf te gaan die zich voordoen bij het op peil houden of brengen van de beveiliging van informatievoorziening. De beschreven auditing-methode gaat uit van de belangrijkste eigendommen van de organisatie (de assets) en centreert het vraagstuk van beveiliging rondom deze assets. Daardoor ontstaat een opdeling in een aantal 'brokken' die te behappen zijn. Bij een grootschalige security-audit ontbreekt deze gewenste fragmentatie. De analyse concentreert zich op één asset of een groep van assets. Dat maakt het ook mogelijk de analyse door meerdere partijen te laten uitvoeren. De domeinmodellen en het stappenplan maken de uitvoering tot een

vastomlijnde procedure. De controle van de beveiliging van een asset kan zo gekoppeld worden aan de eigenaar van de betreffende asset.
De periodieke analyse gaat uit van een kort analyseproces op een beperkt gebied. Daardoor is het ook mogelijk dat de analyse periodiek uitgevoerd wordt en niet beperkt blijft tot een eenmalige audit. Deze periodieke uitvoering is noodzakelijk om de beveiliging doorlopend te kunnen monitoren. Bovendien is de prioriteit van noodzakelijke aanpassingen eenvoudig te bepalen, door middel van het waarderen van de waarde van de assets of assetgroepen.

Het gebruik van de methode staat of valt uiteraard met discipline: alleen regelmatig uitvoeren van de analyse kan zorgen voor voldoende identificatie van de risico's. Ook de afbakening van domein en assets zijn voorwaarde voor succes. Als de verantwoordelijkheden vervolgens goed belegd zijn, staat niets een succesvolle eerste uitvoer in de weg.

Referenties:

[1] David McCoy , *Application Integration and Middleware at the Crossroads*, december 2001.
[2] J. Jaarsma, *Aan de slag met succesvolle risicoanalyses*, IT Beheer Magazine, september 2002.
[3] Ophem van, I., *Security Solutions for the Provider Based Accounting Architecture,* Phd. Faculty of Computer Science, University of Twente, Enschede, Holland, 2001.
[4] Michiels, E.F., *Telematics System Security*, Faculty of Electrical Engineering, University of Twente, Enschede, Holland, 2001.
[5] *Guidelines for the management of IT security (GMITS),* part 3, ISO/IEC TR 13335, 2001.
[6] Breed, N.F., Out, D.J., Tettero, O., *Informatiebeveiliging. Een blik achter de schermen*. Telematica Research Centrum, Enschede 1994.